The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
4/20/2010

SUBJECT:
Vulnerability in HP Operations Manager Could Allow Remote Code Execution

OVERVIEW:
HP has issued a patch to remedy a vulnerability in HP Operations Manager. HP Operations Manager is a management console that correlates data from the network infrastructure. This vulnerability exists in an ActiveX control that will allow an attacker to download malicious files. ActiveX controls are small programs or animations that are downloaded or embedded in websites which will typically enhance functionality and user experience. This vulnerability can be exploited if a user visits or is redirected to a specially crafted webpage hosting a malicious file designed to take advantage of the vulnerability. Successful exploitation may result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Please note: Exploit code is publically available. However, we have not received any reports of active exploitation of this vulnerability.

SYSTEMS AFFECTED:

HP Operations Manager for Windows v8.16
HP Operations Manager for Windows v8.10
HP Operations Manager for Windows v7.5

RISK:

Government:
Large and medium government entities: **High**
Small government entities: **High**

Businesses:
Large and medium business entities: **High**
Small business entities: **High**

Home users: N/A

DESCRIPTION:
A vulnerability has been discovered in the SourceView ActiveX control (srcvw32.dll or srcvw4.dll) of HP Operations Manager that could allow an attacker to execute arbitrary code on an affected system. This issue is caused by a buffer overflow condition in the "srcvw4.dll" or "srcvw32.dll" ActiveX control when processing overly long arguments passed to the "LoadFile()" or "SaveFile()" methods. This vulnerability can be exploited if a user visits or is redirected to a specially crafted website designed to exploit this vulnerability. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

The vulnerability is reported in the following versions:
HP Operations Manager for Windows versions 8.10 and 8.16 with srcvw4.dll version 4.0.1.1 or earlier
HP Operations Manager for Windows version 7.5 with srcvw32.dll version 2.23.28 or earlier

The vulnerable ActiveX controls can be identified by the following Class Identifier (CLSID):
{366C9C52-C402-416B-862D-1464F629CA59}

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by HP to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Ensure that all Microsoft Internet Explorer clients are configured to prompt before executing Active Scripting. If Active Scripting is not required it should be disabled completely.

REFERENCES:
HP:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02078800

Secunia:
http://secunia.com/advisories/39538

Security Focus:
http://www.securityfocus.com/bid/39578

SecureList:
http://www.securelist.com/en/advisories/39538

Vupen:
http://www.vupen.com/english/advisories/2010/0946